FORTINET

LIVRE BLANC

Sécuriser les environnements cloud dynamiques

Développer une liste de contrôle des solutions dans un paradigme en évolution

Le cloud computing a transformé notre façon de consommer et de déployer les solutions informatiques. La puissance de calcul évolue rapidement vers un modèle d'utilité, reposant sur une infrastructure partagée. Cette infrastructure partagée, qui sous-tend la révolution du cloud, a également entraîné un changement fondamental dans la manière dont nous concevons et déployons la technologie au sein du datacenter. Les serveurs, le stockage, les réseaux et même le datacenter lui-même ont dépassé les limites physiques pour devenir des services virtualisés résidant sur du matériel physique. Ce nouveau modèle d'infrastructure partagée virtuelle s'accompagne de nouveaux risques.

Selon IDC, 75 % des entreprises mettent en œuvre un cloud public ou l'envisagent. En outre, IDC prévoit que 50 % des charges de travail des entreprises migreront vers le cloud public d'ici 2018. En parallèle, l'environnement des menaces ne fait que s'étendre, et ce n'est plus le pirate traditionnel pénétrant le périmètre réseau qui stimule ceux qui gèrent la sécurité réseau. Le trafic est-ouest, c'est-à-dire le trafic entre les systèmes à l'intérieur du réseau, domine désormais le flux de données d'entreprise. Les environnements cloud hybrides relient les systèmes et les applications des entreprises aux clients et sources de données externes. Les déploiements de cloudprivés permettent d'augmenter la puissance de calcul en tant que service aux développeurs d'applications qui déploient de nouvelles fonctionnalités à l'intention des utilisateurs internes et externes. Le paradigme de la conception du réseau pour le datacenter est désormais plus plat. Le résultat final est qu'une fois pénétré, le réseau est exposé à des menaces qui peuvent rester cachées, tapies ou dormantes pendant des jours ou des semaines, en attendant le bon moment pour faire des ravages ou voler des données confidentielles. C'est précisément ce type de menace qui pèse lourdement sur les esprits des personnes chargées de la sécurité dans le cloud.

Pour ceux qui cherchent à relever ce défi, nous décrivons ici les éléments clés à prendre en compte dans une solution de sécurité cloud, en gardant à l'esprit que la première règle peut être non seulement de prévenir une violation de données, mais aussi de supposer qu'il y en aura une, et de s'assurer que les éléments d'une solution de sécurité cloud peuvent rester résilients et protégés.

La sécurité dans un cloud public

La sécurité dans un cloud public représente la préoccupation de sécurité la plus importante. Les chefs d'entreprise et les utilisateurs n'ont surmonté que récemment le scepticisme inhérent au partage des systèmes et de la bande passante avec des tiers inconnus. Jusqu'à très récemment, les inquiétudes concernant la sécurité dans le cloud étaient une des raisons pour lesquelles beaucoup tardaient à adopter des options de cloud public. Pour garantir une sécurité efficace dans un cloud public, il faut tenir compte de deux éléments clés : un modèle de sécurité partagé et l'intégration des fournisseurs.

Modèle de sécurité partagé — Le modèle de sécurité partagé doit non seulement être l'approche adoptée par les équipes de sécurité pour sécuriser le cloud, mais les solutions déployées par les entreprises doivent également être suffisamment flexibles pour permettre le déploiement de fonctionnalités de sécurité dans un modèle partagé. Le modèle de sécurité partagé comprend deux éléments clés : la sécurité du cloud, qui inclut tous les composants du datacenter du côté du fournisseur de cloud, et la sécurité dans le cloud, qui consiste en ce que vous, en tant qu'abonné au cloud, êtes responsable de fournir en terme de données et d'applications dans le cloud. Les éléments qui doivent être pris en compte par une solution du côté du client sont les suivants : vos données et applications, les systèmes d'exploitation, la gestion des accès et des identités, le chiffrage et le trafic réseau. Du côté du fournisseur, une solution doit s'intégrer à l'infrastructure de sécurité des fournisseurs de services cloud, qui protège la puissance de calcul, le stockage et le réseau, et fournir un tableau de bord commun pour visualiser les deux côtés et gérer tous les aspects de la solution.

Les réponses à ces questions sur les menaces fourniront aux professionnels de la sécurité un point de départ pour définir les exigences d'une solution de sécurité IoT (Internet-of-Things). La transformation de la frontière IoT en un périmètre renforcé ou, du moins, l'obtention de la visibilité nécessaire pour voir les menaces venir et être en mesure de réagir à une attaque et de la prévenir est la base de toute nouvelle solution.

Intégration des fournisseurs — Au-delà de la définition des domaines de responsabilité et de l'assurance que la protection ne présente aucune lacune, les solutions doivent être étroitement intégrées avec le fournisseur de cloud public pour assurer la sécurité dans le cloud. La sécurité dans le cloud public ne peut pas suivre l'ancien paradigme qui consistait à déployer des solutions basées sur des appliances ou des agents basés sur l'hôte. Ces solutions ne peuvent pas couvrir la visibilité de bout en bout sur tous les nœuds et ne peuvent généralement pas évoluer avec l'élasticité requise pour une solution cloud. Par exemple, les utilisateurs d'Amazon Web Services connaissent le concept de « groupes de sécurité » pour gérer la segmentation de base, mais même AWS recommande d'utiliser la sécurité de tiers pour ajouter des

fonctionnalités comme le contrôle des applications, l'antivirus, le filtrage Web, la protection contre la perte de données et la recherche de menaces. Dans le contexte du cloud public, ces solutions doivent s'adapter automatiquement au cloud, en se basant sur un modèle pour fournir un niveau de haute disponibilité et de performance à mesure que les ressources cloud se développent de manière dynamique. Pour les utilisateurs qui utilisent Microsoft Azure, une solution de sécurité doit intégrer les API afin que Microsoft Azure Resource Manager puisse tirer le meilleur parti des fonctionnalités de sécurité.

La sécurité dans un cloud privé

La virtualisation est à la base du cloud privé. En fait, la virtualisation est la pierre angulaire de toutes les formes de cloud computing. La virtualisation a donné naissance à un environnement informatique plus axé sur les logiciels. C'est cette évolution vers une approche centrée sur les logiciels que toute solution de sécurité cloud doit prendre en compte.

Sécurité définie par logiciel — Avec la croissance des réseaux définis par logiciel (SDN), tout comme le cloud lui-même, les ressources réseau ne sont plus physiquement liées à du matériel dédié. Les ressources réseau fonctionnent comme des services dans le datacenter et, à ce titre, peuvent s'étendre sur des éléments ou des emplacements physiques. Une solution de sécurité cloud doit être conçue dans cette optique, sans qu'il soit nécessaire de déployer des approches de sécurisation des ressources basées uniquement sur des appliances. Les fonctionnalités de sécurité doivent devenir des « services » qui peuvent être configurés et fournis de manière dynamique.

Votre solution répond-elle aux exigences de fonctionnalité des clouds publics, privés et hybrides ?

La sécurité dans un cloud public

- Modèle de sécurité partagé
- Intégration des fournisseurs

La sécurité dans un cloud privé

- Sécurité définie par logiciel
- Sécurité centrée sur les applications

Le cloud hybride

- Gestion via une interface unique
- Segmentation
- Connectivité sécurisée

Sécurité centrée sur les applications — Toutes les applications ne sont pas créées égales. Si beaucoup d'entre elles partagent la même infrastructure physique dans un cloud privé, elles ne présentent pas le même profil de risque. Par conséquent, la segmentation est essentielle et la solution de sécurité doit être alignée sur l'application. Toute solution de sécurité cloud doit être capable d'isoler les données et les applications au fur et à mesure que le datacenter se consolide. Comme le trafic est-ouest augmente dans les environnements définis par logiciel, la micro-segmentation, c'est-à-dire la capacité à segmenter des types de trafic spécifiques, devient également cruciale.

Le cloud hybride

Le cloud hybride présente peut-être le problème le plus difficile à résoudre lorsqu'il s'agit de déterminer la meilleure solution de sécurité. Avec des ressources couvrant à la fois les actifs que vous contrôlez et l'infrastructure de cloud public ou des ressources de données ou SaaS spécifiques, la visibilité est primordiale pour que l'équipe de sécurité ait une visibilité complète de bout en bout. La gestion de bout en bout, la segmentation et la sécurisation des connexions externes deviennent les éléments les plus importants d'une solution de sécurité cloud hybride.

Gestion via une interface unique — Les ressources étant réparties entre le domaine physique et le domaine virtuel, les professionnels de la sécurité ne peuvent pas constamment alterner les tableaux de bord pour obtenir une visibilité complète, ni opérer sans analyse centralisée pour pouvoir exploiter les renseignements sur les menaces. Des solutions individuelles dotées d'interfaces de gestion séparées ne suffisent pas. Une solution de sécurité cloud doit intégrer une vue unique de tous les systèmes fonctionnant dans le cloud avec une gestion centralisée. Cette approche de gestion via une interface unique doit vous permettre de suivre les flux de données sur l'ensemble du réseau dans un format qui rend ces informations pertinentes et exploitables. Elle doit également comprendre un système centralisé de renseignements sur les menaces, permettant de prendre des décisions en fonction de ce qui se passe sur votre réseau et à l'extérieur.

Segmentation — La segmentation des systèmes et du trafic dans et à travers le cloud est particulièrement cruciale lorsque les ressources internes se trouvent sur un réseau ouvert au public ou à des tiers. Dans ces environnements intrinsèquement mixtes qui comprennent à la fois des connexions externes permanentes et des mouvements de données temporaires, les divisions opérationnelles et les applications essentielles qui ne sont pas directement associées à l'environnement hybride doivent être segmentées pour minimiser l'impact en cas de violation.

Connectivité sécurisée — Toute solution hybride doit offrir une fonctionnalité VPN robuste, qui permet notamment de fournir un accès temporaire sécurisé aux ressources, au besoin, tout en protégeant le reste du réseau. La migration des données entre les sites, le chargement de grands ensembles de données provenant de sources externes, l'utilisation de services d'analyse cloud tiers, tout cela nécessite des connexions discrètes à des réseaux externes qui comportent des risques uniques. Une solution doit être capable de fournir la protection adéquate en fonction du profil de risque de ces connexions réseau uniques.

Une sécurité adaptée au paradigme du cloud

En plus de protéger le cloud dans ses différents déploiements, public, privé et hybride, une solution de sécurité cloud doit également s'adapter à la nature du cloud lui-même, en tant que ressource élastique et dynamique qui peut évoluer rapidement. La solution doit tenir compte de trois aspects clés du cloud.

Évolutivité — Étant donné que le cloud est dynamique et que l'évolutivité est le principal facteur qui pousse de nombreux utilisateurs à déplacer des solutions vers le cloud, la conception d'une solution de sécurité doit s'adapter à l'évolutivité et l'élasticité des charges de travail dans le cloud. Les solutions qui sont statiques ou manquent d'automatisation, nécessitant une intervention pour étendre ou adapter de nouvelles exigences, font de la sécurité un obstacle à la pleine exploitation des solutions cloud. Lors de l'évaluation d'une solution de sécurité cloud, l'automatisation doit être au cœur de la solution. Les politiques de risque et d'accès doivent également être définies à l'avance de façon à ce que les nouveaux appareils qui entrent sur le réseau pour accueillir plus d'utilisateurs ou une bande passante supplémentaire dans l'environnement cloud soient automatiquement configurés. La solution peut-elle s'adapter à l'élasticité et la croissance dynamique d'un environnement cloud ?

Cohérence — Les menaces se développent en trouvant la bonne opportunité au bon moment. Souvent, cela signifie qu'il faut exploiter les incohérences des politiques ou de leur application pour pénétrer dans votre réseau. Le cloud exige ainsi un nouveau niveau de cohérence. Le cloud introduit de nouvelles variables telles que les connexions temporaires ou récurrentes à des ressources extérieures, et l'extension et la contraction dynamiques des ressources en fonction de la demande. La politique, l'application et l'automatisation qui exécute les deux doivent être mises en œuvre de manière cohérente dans les ressources statiques et dynamiques. Les charges de travail ou les systèmes classés selon un profil de risque commun doivent être traités de la même manière lorsqu'ils entrent ou sortent du réseau, qu'ils se trouvent dans votre datacenter ou chez vos fournisseurs. Pouvez-vous maintenir une cohérence en matière d'application des politiques, devisibilité et de protection dans le cloud ?

Segmentation — Qu'il s'agisse de minimiser les risques opérationnels ou de répondre aux exigences réglementaires, le cloud introduit de nouveaux éléments dans le protocole de sécurité. La capacité à segmenter les systèmes, les charges de travail ou même des composants réseau spécifiques est essentielle pour gérer les risques opérationnels. Le cloud présente également de nouveaux risques pour la conformité. Lorsque des données peuvent non seulement transiter par votre réseau mais aussi le quitter via le cloud public, la conformité des données doit être appliquée de façon à garantir la surveillance et le contrôle d'un trafic, d'applications ou de types de données spécifiques. Une bonne segmentation des solutions cloud permet également d'inspecter le trafic persistant entre les segments du cloud afin d'assurer une protection contre les fuites de données et l'acheminement des données en fonction des risques et des politiques. Pouvez-vous séparer les systèmes, les charges de travail et les applications essentiels en fonction de profils de risque uniques ?

Votre solution est-elle adaptée au paradigme de la sécurité dans le cloud ?

Évolutivité

La solution peut-elle s'adapter à l'élasticité et la croissance dynamique d'un environnement cloud ?

Cohérence

Pouvez-vous maintenir une cohérence en matière d'application des politiques, de visibilité et de protection dans le cloud ?

Segmentation

Pouvez-vous séparer les systèmes, les charges de travail et les applications essentiels en fonction de profils de risque uniques ?

Conclusion

Le cloud computing a transformé le paradigme des professionnels de l'informatique et de la sécurité. L'époque où les réseaux avaient des périmètres bien définis et où la protection se concentrait uniquement sur les menaces externes tentant de contourner le pare-feu, est révolue. Les solutions de sécurité cloud doivent répondre aux exigences uniques de chaque variante du cloud computing : le cloud public, avec sa dépendance à l'égard des infrastructures partagées et la nécessité de fonctionner dans un modèle de sécurité partagé ; le cloud privé, avec les risques inhérents au trafic est-ouest et aux services virtualisés qui requièrent une approche de la sécurité définie par logiciel ; le cloud hybride, qui présente le défi de combiner les ressources internes essentielles avec des connexions et des sources de données externes, augmentant ainsi le besoin de segmenter les ressources sur le réseau.

En parallèle, une solution doit s'adapter à l'évolutivité du cloud, en appliquant et en mettant en œuvre les politiques de manière cohérente dans des ressources segmentées, tant en interne qu'en externe. Grâce à cette combinaison de fonctionnalités et d'approches, une solution peut relever les défis de la sécurité dans le cloud tout en permettant à l'entreprise de profiter des avantages du cloud et de minimiser les risques opérationnels de l'infrastructure publique partagée.

FORTINET®

www.fortinet.fr

juillet 20, 2020 4:29 PM

122915-B-0-FR

wp-FA-securing-dynamic-cloud-environments_FR